REMARKS

This amendment is responsive to the Office Action dated September 29, 2004. Applicants have amended claims 1-9, 11, 12, 14-20 and added claims 22-28. Claims 1-28 are pending upon entry of this amendment.

Claim Objections

In the Office Action, the Examiner objected to claims 1, 5 and 11. Applicants have amended claims 1, 5 and 11 for purposes of clarification.

Claim Rejection Under 35 U.S.C. § 102

Claims 1-7, 9 and 10

In the Office Action, the Examiner rejected claims 1-7, 9 and 10 under 35 U.S.C. 102(e) as being anticipated by Devine et al. (US 6,606,708 B1). Applicants respectfully traverse the rejection. Devine et al. fails to disclose each and every feature of the claimed invention, as required by 35 U.S.C. 102(e), and provides no teaching that would have suggested the desirability of modification to include such features.

For example, Devine et al. (Devine) fails to teach or suggest a load balancing acceleration device that comprises both an encryption and decryption engine and a load balancing engine, as recited by Applicants' claim 1. In particular, Devine fails to teach or suggest a device that comprises both (i) an encryption and decryption engine instructing a processor to decrypt data received via the secure communication session and direct the decrypted data to one of a plurality of server devices via a second communication session, and (ii) a load balancing engine associating each of said client devices with a respective one of said server devices based on calculated processing loads of each said server devices.

In contrast, Devine describes a "double firewalled" system having a first firewall, a plurality of web servers, a second firewall and a plurality application servers. None of the devices described by Devine operate as an acceleration device that includes both an encryption and decryption engine and a load balancing engine that associates each of the client devices with a respective server based on calculated processing loads of each server. Rather, the Devine system includes describe a plurality of web servers 24 that essentially act as secure relay devices.

More specifically, web servers 24 located within a Demilitarized Zone (DMZ) communicate with client devices via a first set of secure communications sessions (e.g., HTTPS), and relay requests to appropriate application servers 40 located within the enterprise via a dispatcher server 26.

In rejecting claim 1, the Examiner specifically cited column 8, lines 22-65 of Devine. In the cited portions, however, Devine refers to Figure 4 and describes web servers 24 as utilizing SSL and HTTPS to relay communications between client devices and application servers 40 via secure TCP messaging sessions. For example, the cited portion of Devine specifically states that web servers 24 receive messages from client devices S-HTTP or HTTPS, and then forwards the requests to dispatcher server 26 located inside the enterprise Intranet. According to Devine, dispatcher 26 re-encrypts the messages and forwards the messages to the "appropriate" application server based on the service specifically requested by the client. In other words, dispatcher 26 forwards the message to the application server 40 that provides the requested service, e.g., electronic mail, broadband, service inquiries and other services.

Thus, it is clear that neither web servers 24 nor dispatcher 26 of the Devine system include a load balancing engine that associates each of said client devices with a respective one of said servers based on calculated processing loads of each said server, as required by Applicants' claim 1. Consequently, none of the devices of the Devine system comprises both an encryption and decryption engine for providing secure communications and a load balancing engine, as recited by Applicants' claim 1. In fact, it appears the only device within the Devine system that performs any form of load balancing is the "HydraWeb Load Balancer 45" depicted in Figure 4 and further described in column 23. However, as clearly shown in Figure 4, this device is a dedicated switching unit that does not comprise both an encryption and decryption engine and a load balancing engine, as recited by Applicants' claim 1.

Further, Devine fails to teach or suggest a load balancing acceleration device that comprises a TCP communications manager capable of interacting with a plurality of client devices and server devices simultaneously via the communications interface, and a secure communications manager to negotiate a secure communication session with one of the client devices, wherein the TCP communications manager provides an IP address of an enterprise to said secure communications manager, and each of said plurality of server devices is associated with the enterprise, as recited by Applicants' claim 2.

In rejecting claim 2, the Examiner refers to col. 23, ln. 17 to col. 24, ln. 14. However, this section of Devine merely describes the conventional HydraWeb Load Balancer 45. Thus, in rejecting Applicants' claim to an acceleration device, the Examiner appears to erroneously attribute load-balancing functions from the HydraWeb Load Balancer 45 to other devices of the Devine system. Neither web servers 24, dispatcher 26 nor the HydraWeb Load Balancer 45 of the Devine system teach or suggest an acceleration device that includes both an encryption and decryption engine for providing secure communications and a load balancing engine that associates each of said client devices with a respective one of said servers based on calculated processing loads of each said server, wherein the acceleration device includes a TCP communications manager that provides an IP address of an enterprise to said secure communications manager, as required by claim 2.

Devine fails to teach or suggest a load balancing acceleration device that comprises a secure communications manager that negotiates a secure communication session with each of said plurality of client devices over an open network, and a TCP communications manager that negotiates a separate, open communications session with one of the plurality of server devices associated with the enterprise for each secure communication session negotiated with the client devices based on the associations of said client devices to said server devices by said load balancing engines, as required by Applicants' claims 3 and 4.

In contrast to the Examiner's assertions, the Devine system fails to describe a device that negotiates secure communication session with client devices and respective open (non-secure) communications sessions to servers. Rather, Devine makes clear that web servers 24 essentially act as secure relay devices. More specifically, web servers 24 located within a Demilitarized Zone (DMZ) communicate with client devices via a first set of secure communications sessions (e.g., HTTPS), and relay communications to appropriate application servers 40 located within the enterprise via a dispatcher server 26 and a second set of secure communications.

Thus, the Examiner's analysis in rejecting in claims 3 and 4 is flawed for at least two reasons. First, in the Devine system, communications are relayed using two sets of secure communication sessions. Thus, no device in the Devine system is actually operating as an acceleration device on behalf of another device and, therefore, no device negotiates secure communication sessions with the client devices and negotiates open communications session with server devices, as required by Applicants' claims. Second, there is no indication of a one-to-one mapping in the Devine system between secure communication sessions from the client devices to the acceleration device and the open (non-secure) communication sessions from the acceleration device to the server device as required by Applicants' claims 4 and 9.

Applicants have amended claim 5 to clarify that, unlike conventional SSL accelerators, the claimed acceleration device performs encryption and decryption on the packet level. In particular, Applicants have amended claim 5 to require that the encryption and decryption engine decrypt the data on a packet level by decrypting packet data received via the secure communication session to extract a secure record, decrypting application data from the secure record in the packet data, and outputting the decrypted application data from the secure record to the one of said server devices via the second communication session without processing the application data with an application layer of a TCP/IP stack.

For purposes of clarity, Applicants refer the Examiner to Figure 2B and pages 5 and 6 that describe conventional SSL acceleration devices and, in particular, how in prior art systems HTTP packets conventionally traverse the entire networking protocol stack including the IP layer, the SSL session layer and the application layer multiple times.

In contrast, embodiments of the present invention include an acceleration device that operates at the packet level. Applicants refer the Examiner to page 10, ll. 3-13 of the present application that states:

> *Figure 3 shows how the system of the present invention differs in general from that of the prior art, and illustrates the manner in which the SSL encryption and decryption proxy is implemented. Typically, when a Web client wishes to send data via a secure protocol to an SSL enabled Web server, it will do so by communicating via a secure port 443. As shown in Figure 3, in accordance with the present invention, the SSL accelerator will intercept data destined for port 443 of the web server and, rather than the transmitting packets up and down the TCP/IP stack as shown in Figure 2B, will perform the SSL encryption and decryption at the packet level before forwarding the packet on to its destination. The accelerator will thus decode the packet data and forward a clear text (HTTP) packet the HTTP port 80 of the Web server 300.*

Further, on page 16, ll. 17-26, the present application states that:

> *As shown at reference number 265, client 100 will now begin sending encrypted application data to the SSL accelerator device 250. ... The accelerator device will process the data at step 270 on the packet level and forward it to the server as clear text.*

Devine fails to teach or suggest an acceleration device having an encryption and decryption engine that decrypts the data on a packet level by decrypting packet data received via the secure communication session to extract an SSL record, decrypting application data from the SSL record in the packet data, and outputting the decrypted application data from the SSL record to the one of said server devices via the second communication session without processing the application data with an application layer of a TCP/IP stack, as required by claim 5 as amended.

In contrast, the Devine system describes web servers 24 as implementing HTTPS, which operates at the application layer (HTTP) and the session layer (SSL). Devine specifically describes decrypting and re-encrypting messages and forwarding the messages via HTTP. Thus, Devine does not describe an SSL acceleration device that operations on the packet-level as described and claimed by the Applicants.

Devine et al. fails to disclose each and every limitation set forth in claims 1-7, 9 and 10. For at least these reasons, the Examiner has failed to establish a prima facie case for anticipation of Applicants' claims 1-7, 9 and 10 under 35 U.S.C. 102(e). Withdrawal of this rejection is requested.

Claims 12-15 and 17-21

In the Office Action, the Examiner rejected claims 12-15 and 17-21 under 35 U.S.C. 102(e) as being anticipated by Lincke et al. (US 6,397,259 B1). Applicants respectfully traverse the rejection to the extent such rejection may be considered applicable to the amended claims. Lincke et al. fails to disclose each and every feature of the claimed invention, as required by 35 U.S.C. 102(e), and provides no teaching that would have suggested the desirability of modification to include such features.

Applicants have amended claim 12 to clarify that the steps are performed within an intermediate acceleration device enabled for communication between a plurality of customer devices and a plurality of servers of an enterprise. With respect to claim 12, Lincke fails to teach or suggest receiving with an acceleration device communications directed to the enterprise in a secure protocol from the customer devices, decrypting data packets of the secure protocol with the acceleration device to provide decrypted packet data, selecting with the acceleration device at least one of the plurality of servers in the enterprise based on a load calculation including processing sessions of other servers in the enterprise and associating the selected server with a communications session from the one of the clients, and forwarding the decrypted packet data from the acceleration device to the selected server of the enterprise.

In general, Lincke describes a wireless communication system that utilizes data compression techniques and appears to generally be irrelevant to Applicants' claims. The Lincke system includes a proxy device that utilizes a security protocol when communicating with a wireless client. In the cited portions, Lincke merely states that statistics on usage patterns may be collected for the communications, and that the proxy server itself may be shared on two or more machines for load balancing. Moreover, at col. 86, ln. 15, Lincke makes clear that the proxy server itself forms responses to the wireless clients.

Thus, Lincke fails to describe decrypting data packets with an intermediate acceleration device, selecting with the acceleration device at least one of the plurality of servers in the enterprise based on a load calculation, and forwarding the decrypted packet data from the acceleration device to the selected server of the enterprise, as required by claim 12 as amended. In fact, Lincke fails to describe any form of actively load balancing decrypted packet data across servers at all.

With respect to claim 14, Devine Lincke fails to teach or suggest receiving with the device communications having a destination IP address of the enterprise. In the portion cited by the Examiner, Lincke merely states that a wireless interface determines whether an incoming packet is destined for an IP address of the proxy server to determine whether to compress the packet. Lincke does not describe receiving communications directed to an enterprise.

With respect to claim 17, Lincke fails to teach or suggest establishing an open communication session from the acceleration device to the selected server, and mapping the decrypted packet data to the open communications session established with the selected server. The portion cited by the Examiner (i.e., col. 85 ln. 63 to col. 86 ln. 20) describes a symmetric key decryption process utilized by the Lincke wireless communication system. In relevant part, Lincke states that the proxy server forms a response and then encrypts the response using symmetric encryption algorithm (col. 86, ln. 15). Thus, the Examiner's analysis is incorrect for at least two reasons. First, Lincke does not describe an open (non-secure) communication session at all. Second, Lincke does not teach or suggest forwarding the decrypted data to one or a plurality of servers at all, let alone over an open communication system. To the contrary, it appears the proxy server 180 of the Lincke system forms responses for transmission to the client devices and, therefore, does not forward the decrypted data to a plurality of servers over open communication sessions.

With respect to claim 19, the Examiner has misconstrued Lincke and overlooked many of the Applicants' claim elements. For example, claim 19 recites receiving encrypted data having a length greater than a TCP segment carrying said data, and wherein said step of decrypting comprises: buffering the encrypted data in a memory buffer in the accelerator device, the buffer having a length equivalent to the block cipher size necessary to perform the cipher; and decrypting the buffered segment of the received encrypted data to provide decrypted application data.

Contrary to the Examiner's assertion, Lincke makes no mention of these novel features. In fact, the cited portion of Lincke makes a passing reference to SSL and specifically states that the wireless communication system specifically does not even utilize SSL. Clearly, Lincke does not teach or suggest the novel claim elements recited by claim 19. Applicants respectfully request examination of claim 19 on the merits.

Similarly, with respect to claim 20, the Applicants have amended claim 20 to clarify that the data is authenticated on a packet level on receipt of a final TCP segment without processing the application data with an application layer of a TCP/IP stack. Lincke fails to teach or suggest these requirements. To the contrary, the cited portion of Lincke clearly states that "the wireless communications system provides neither wireless client 405 authentication, nor nonrepudication. Some level of wireless client 405 authentication and nonrepudiation is provided by the application layer." Thus, Lincke makes clear that authentication does not occur below the application level, as described and claim by the Applicants.

Lincke et al. fails to disclose each and every limitation set forth in claims 12-15 and 17-21. For at least these reasons, the Examiner has failed to establish a prima facie case for anticipation of Applicants' claims 12-15 and 17-21 under 35 U.S.C. 102(e). Withdrawal of this rejection is requested.

Claim Rejection Under 35 U.S.C. § 103

In the Office Action, the Examiner rejected claims 8 and 11 under 35 U.S.C. 103(a) as being unpatentable over Devine in view of Gelman et al. (US 6,415,329 B1), and rejected claim 16 under 35 U.S.C. 103(a) as being unpatentable over Lincke as applied to claim 12 above, and further in view of Gelman. Applicants respectfully traverses the rejection. Gelman et al. (Gelman) fails to disclose or suggest the inventions defined by Applicants' claims, and provide no teaching that would have suggested the desirability of modification to arrive at the claimed invention.

In general, Gelman describes a method of communicating over a satellite or other high delay-bandwidth link. Gelman describes modifying destination address in a first protocol, forwarding the packets in a second protocol and then restoring the destination address (Abstract).

With respect to claims 8, 11 and 16, the Examiner states that it would have been obvious to a person having ordinary skill in the art to modify the proxy server of Devine to change the IP addresses. This analysis is flawed for at least two reasons.

First, Devine does not describe a proxy server. Applicants assume the Examiner incorrectly referred to Devine, and instead meant to refer to the proxy server described in Lincke. Applicants assume for purposes of this response that the Examiner is referring to the proxy server of Lincke.

Second, as described above, Lincke does not teach or suggest forwarding the decrypted data to one or a plurality of servers at all. To the contrary, the proxy server 180 of the Lincke system forms and issues responses to the wireless client devices and, therefore, does not forward the decrypted data to a plurality of servers at all. Consequently, the Examiner assertion that the proxy server could somehow be modified to modify IP addresses of destination servers is incorrect.

For at least these reasons, the Examiner has failed to establish a prima facie case for non-patentability of Applicants' claims 8, 11 and 16 under 35 U.S.C. 103(a). Withdrawal of this rejection is requested.

New Claims:

Applicants have added claims 22-28 to the pending application. The applied references fail to disclose or suggest the inventions defined by Applicants' new claims, and provide no teaching that would have suggested the desirability of modification to arrive at the claimed inventions.

As one example, the cited references fail to teach or suggest a network router that operates as a load-balancing acceleration device as required by claim 22.

As another example, the references fail to teach or suggest decrypting the data packets to extract a secure record, decrypting application data from the secure record, and authenticating the application data without processing the application data with an application layer of a TCP/IP stack, as required by Applicants new claim 24.

As another example, the references fail to teach or suggest a system comprising a client device, a plurality of server devices and an intermediate device coupled between the client devices and the server devices, wherein the intermediate device intercepts a request from the client device for a secure communication session, and wherein, in response to the request, the intermediate establishes a secure communication session with the client device, selects one of the server devices based on resource loading experienced by the server devices, and establishes a non-secure communication session with the selected server device, as required by Applicants' new independent claim 25.

No new matter has been added by the new claims.

CONCLUSION

All claims in this application are in condition for allowance. Applicants respectfully request reconsideration and prompt allowance of all pending claims. Please charge any additional fees or credit any overpayment to deposit account number 50-1778. The Examiner is invited to telephone the below-signed attorney to discuss this application.

Date:

January 11, 2005

SHUMAKER & SIEFFERT, P.A.
8425 Seasons Parkway, Suite 105
St. Paul, Minnesota 55125
Telephone: 651.735.1100
Facsimile: 651.735.1102

By:

Name: Kent J. Sieffert
Reg. No.: 41,312